TO: USPTO

ZILKA·KOTAB PC

ZILKA, KOTAB & FEECE™

100 PARK CENTER PLAZA, SUITE 300
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	November 22, 2006	**Phone Number**	**Fax Number**
To:	Board of Patent Appeals		(571) 273-8300
From:	Kevin J. Zilka		

Docket No.: NAI1P456/00.163.01 **App. No: 09/785,222**

Total Number of Pages Being Transmitted, Including Cover Sheet: 43

Message:

Please deliver to the Board of Patent Appeals.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Erica
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

November 22, 2006

RECEIVED
CENTRAL FAX CENTER

NOV 22 2006

Practitioner's Docket No. NAI1P456/00.163.01 ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Tarbotton et al.

Application No.: 09/785,222
Filed: 02/20/2001
For: SOFTWARE AUDIT SYSTEM

Group No.: 2131
Examiner: Chai, L.

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal, filed in this case on 08/08/2006, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review, mailed 10/24/2006.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*

(When using Express Mail, the Express Mail label number is mandatory; Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ **(mandatory)**

TRANSMISSION

✓ _ facsimile transmitted to the Patent and Trademark Office, (571) 273 - 8300.

Date: 11/22/06

Signature

Erica L. Farlow

(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

RECEIVED
CENTRAL FAX CENTER
NOV 2 2 2006

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$500.00**

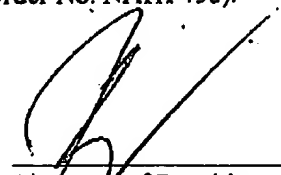
6. FEE PAYMENT

Authorization is hereby made to charge the amount of $500.00 to Deposit Account No. 50-1351 (Order No. NAI1P456).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P456).



Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Tarbotton et al.	Group Art Unit: 2131
Application No. 09/785,222	Examiner: Chai, Longbit
Filed: 02/20/2001	Date: 11/22/2006
For: SOFTWARE AUDIT SYSTEM	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on 08/08/2006, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review, mailed 10/24/2006.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

VII ARGUMENT

VIII CLAIMS APPENDIX

IX EVIDENCE APPENDIX

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-5, 7, 8, 10-23, 25, 26, 28-41, 43, 44, 46-54, and 58-61

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-5, 7, 8, 10-23, 25, 26, 28-41, 43, 44, 46-54, and 58-61
3. Claims allowed: None
4. Claims rejected: 1-5, 7, 8, 10-23, 25, 26, 28-41, 43, 44, 46-54, and 58-61
5. Claims cancelled: 6, 9, 24, 27, 42, 45, and 55-57

C. CLAIMS ON APPEAL

The claims on appeal are: 1-5, 7, 8, 10-23, 25, 26, 28-41, 43, 44, 46-54, and 58-61

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 1-5, a computer program product is provided which includes a computer program operable to control a computer to generate audit data indicative of a request to execute a computer program. The computer program includes computer virus scanner logic (e.g. see item 16 of Figure 2, etc.) which is responsive to a computer virus scan request including data identifying a computer file to be scanned for computer viruses (e.g. see item 28 of Figure 3, etc. The computer virus scanner logic is operable for performing a computer virus scan (e.g. see item 42 of Figure 4, etc.) and for generating a scan result.

In addition, the computer program includes audit data generator logic (e.g. see item 18 of Figure 2, etc.) separate from the computer virus scanner logic. The audit data generator logic is triggered by the computer virus scanner logic prior to the generating the scan result. The audit data generator logic is responsive to the data identifying the computer file to be scanned that is received from the computer virus scanner logic for simultaneously performing additional operations in parallel with the computer virus scan. The additional operations include identifying a request to execute a computer program associated with the computer file to be scanned for computer viruses by the computer virus scanner logic and, in response to identification of the request to execute the computer program, generating audit data identifying the computer program (e.g. see item 62 of Figure 5, etc.).

Additionally, the computer program includes concurrent usage logic for performing a concurrent usage check (e.g. see item 72 of Figure 5, etc.) for identifying a request to execute a further computer program that would result in the further computer program concurrently executing upon more than a predetermined number of computers upon a computer network (e.g. see item 2 of Figure 1, etc.). The predetermined number varies with time. See, for example, page 1 line 22-page 2, line 8; and page 3, line 22-page 4, line 9 et al.

With respect to a summary of Claim 19, as shown in Figures 1-5, a method is provided for generating audit data indicative of a request to execute a computer program. In use, a computer

virus scan is performed and a scan result is generated (e.g. see item 32 of Figure 3, etc.) in response to a computer virus scan request within a computer virus scanner (e.g. see item 28 of Figure 3, etc.). The computer virus scan request includes data identifying a computer file to be scanned for computer viruses (e.g. see item 38 of Figure 4, etc.).

In addition, operation of an audit data generator (e.g. see item 18 of Figure 2, etc.) which is separate from the computer virus scanner (e.g. see item 16 of Figure 2, etc.) is triggered, using the computer virus scanner prior to generating the scan result. The audit data generator is responsive to the data identifying the computer file to be scanned that is received from the computer virus scanner (e.g. see item 58 of Figure 5, etc.) for simultaneously performing additional operations in parallel with the computer virus scan. The additional operations include identifying a request to execute a computer program associated with the computer file to be scanned for computer viruses by the computer virus scanner.

Additionally, in response to identification of the request to execute the computer program, audit data identifying the computer program is generated (e.g. see item 62 of Figure 5, etc.), and a concurrent usage check is performed (e.g. see item 72 of Figure 5, etc.) for identifying a request to execute a further computer program that would result in the further computer program concurrently executing upon more than a predetermined number of computers upon a computer network (e.g. see item 2 of Figure 1, etc.). The predetermined number varies with time. See, for example, page 3, line 22-page 4, line 9; and page 5 lines 4-14 et al.

With respect to a summary of Claim 37, as shown in Figures 1-5, an apparatus is provided for generating audit data indicative of a request to execute a computer program (e.g. see Figure 2, etc.). The apparatus includes a computer virus scanner (e.g. see item 16 of Figure 2, etc.), responsive to a computer virus scan request (e.g. see item 28 of Figure 3, etc.), for performing a computer virus scan (e.g. see item 42 of Figure 4, etc.) and for generating a scan result. The computer virus scan request includes data identifying a computer file to be scanned for computer viruses.

Further, the apparatus includes an audit data generator (e.g. see item 18 of Figure 2, etc.) separate from the computer virus scanner (e.g. see item 16 of Figure 2, etc.). The audit data generator is

triggered by the computer virus scanner prior to generating the scan result, and is responsive to the data identifying the computer file to be scanned that is received from the computer virus scanner for simultaneously performing additional operations in parallel with the computer virus scan. The additional operations include identifying a request to execute a computer program associated with the computer file to be scanned for computer viruses by the computer virus scanner and, in response to identification of the request to execute the computer program, generating audit data identifying the computer program (e.g. see item 62 of Figure 5, etc.).

In addition, the apparatus includes a concurrent usage monitor for performing a concurrent usage check (e.g. see item 72 of Figure 5, etc.) for identifying a request to execute a further computer program that would result in the further computer program concurrently executing upon more than a predetermined number of computers upon a computer network (e.g. see item 2 of Figure 1, etc.). The predetermined number varies with time. See, for example, page 1 line 22-page 2, line 8; and page 3, line 22-page 4, line 9 et al.

Of course, the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has objected to the specification as failing to provide proper antecedent basis for the claimed subject matter.

Issue # 2: The Examiner has rejected Claims 1, 19, and 37 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

Issue # 3: The Examiner has rejected Claim 1 under 35 U.S.C. 101, as being directed toward non-statutory subject matter.

Issue # 4: The Examiner has rejected Claims 1, 7, 8, 10-12, 15, 19, 25, 26, 28-30, 33, 37, 43, 44, 46-48, 51, and 58-61 under 35 U.S.C. 103(a) as being unpatentable over Chi (U.S. Patent No. 6,006,329), in view of Farber et al. (U.S. Patent No. 6,415,280), and further in view of Greschler et al. (U.S. Publication No. 2002/0078203).

Issue # 5: The Examiner has rejected Claims 2-5, 20-23, and 38-41 under 35 U.S.C. 103(a) as being unpatentable over Chi (U.S. Patent No. 6,006,329), in view of Farber et al. (U.S. Patent No. 6,415,280), in view of Greschler et al. (U.S. Publication No. 2002/0078203), and further in view of Chambers (U.S. Patent No. 5,398,196).

Issue # 6: The Examiner has rejected Claims 13, 14, 17, 18, 31, 32, 35, 36, 49, 50, 53, and 54 under 35 U.S.C. 103(a) as being unpatentable over Chi (U.S. Patent No. 6,006,329), in view of Farber et al. (U.S. Patent No. 6,415,280), in view of Greschler et al. (U.S. Publication No. 2002/0078203), and further in view of Hypponen et al. (U.S. Patent No. 6,577,920).

Issue # 7: The Examiner has rejected Claims 17, 18, 35, 36, 53, and 54 under 35 U.S.C. 103(a) as being unpatentable over Chi (U.S. Patent No. 6,006,329), in view of Farber et al. (U.S. Patent No. 6,415,280), in view of Greschler et al. (U.S. Publication No. 2002/0078203), and further in view of Schlossberg et al. (U.S. Publication No. 2002/0066034).

Issue # 8: The Examiner has rejected Claims 16, 34, and 52 under 35 U.S.C. 103(a) as being unpatentable over Chi (U.S. Patent No. 6,006,329), in view of Farber et al. (U.S. Patent No. 6,415,280), in view of Greschler et al. (U.S. Publication No. 2002/0078203),, and further in view of Bates et al. (U.S. Patent No. 6,721,721).

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has objected to the specification as failing to provide proper antecedent basis for the claimed subject matter.

In particular, the Examiner has objected to the specification as allegedly failing to provide proper antecedent basis for the claimed "data ... received from said computer virus scanner logic for simultaneously performing additional operations in parallel with said computer virus scan, said additional operations including identifying a request to execute a computer program associated with said computer file to be scanned for computer viruses by said computer virus scanner logic."

Appellant respectfully disagrees with such objection and points out that, in response to operation 40 of Figure 4, Figure 5 is carried out simultaneously and in parallel with subsequent operations 42-50 of Figure 4 that follow operation 40, as further evidenced by the detailed description of such figures et al. (e.g. see the Examiner's citation, etc.). Of course, such citations (in combination with the remaining specification) are merely examples of the above claim language and should not be construed as limiting in any manner.

Issue # 2:

The Examiner has rejected Claims 1, 19, and 37 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

Group #1: Claims 1, 19, and 37

Appellant respectfully disagrees with the rejection for the reasons argued above with respect to Issue #1.

Issue # 3:

The Examiner has rejected Claim 1 under 35 U.S.C. 101, as being directed toward non-statutory subject matter.

Group #1: Claim 1

The Examiner has argued that appellant's "claimed subject matter is merely drawn to computer programs claimed as computer listings per se (as a computer program product or a software product)." Appellant respectfully disagrees with the rejection, and asserts that the preamble of Claim 1 positively recites "a computer program operable to control a computer" (emphasis added), as claimed by appellant. Thus, a physical medium is provided for the computer program product of Claim 1.

Issue # 4:

The Examiner has rejected Claims 1, 7, 8, 10-12, 15, 19, 25, 26, 28-30, 33, 37, 43, 44, 46-48, 51, and 58-61 under 35 U.S.C. 103(a) as being unpatentable over Chi (U.S. Patent No. 6,006,329), in view of Farber et al. (U.S. Patent No. 6,415,280), and further in view of Greschler et al. (U.S. Publication No. 2002/0078203).

Group #1: Claims 1, 7, 8, 10-12, 15, 19, 25, 26, 28-30, 33, 37, 43, 44, 46-48, and 51

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of

success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the *prima facie* case of obviousness and, in particular, the obviousness of combining the Chi and Farber references, the Examiner argues that "[i]t would have been obvious...to combine the teaching of Farber within the system of Chi because (a) Chi teaches a method of computer virus detection (Chi: see for example, Column 1 Line 6-7) and (b) Farber teaches an improved virus check of security method by validating the file integrity (Farber: see for example, Column 3 Line 38-42 and Column 6 Line 37-40)." Appellant respectfully asserts that it would not have been obvious to combine the teachings of the Chi and Farber references, especially in view of the vast evidence to the contrary.

For example, Chi relates to detecting computer viruses, while Farber relates to content delivery. To simply glean features from a virus detection system, such as that of Chi, and combine the same with the *non-analogous art* of content delivery systems, such as that of Farber, would simply be improper. Virus detection systems detect viruses in data, while content delivery systems simply deliver content in response to requests for the content. "In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992) In view of the vastly different types of problems a virus detection system addresses as opposed to a content delivery system, the Examiner's proposed combination is inappropriate.

More importantly, appellant respectfully asserts that the third element of the *prima facie* case of obviousness has also not been met. For example, with respect to the independent claims, the Examiner has relied Col. 3, lines 17-23 from Chi to make a prior art showing of appellant's claimed "audit data generator logic separate from said computer virus scanner logic and being triggered by said computer virus scanner logic prior to said generating said scan result" (see this or similar, but not necessarily identical language in the independent claims).

Appellant respectfully asserts that the excerpt from Chi relied upon by the Examiner merely teaches what steps are taken "[w]hen the processor 110 receives a request to scan files for viruses" (Col. 3, lines 17-18 - emphasis added). Specifically, the processor "... sends a request to the storage medium 130 to retrieve the data streams associated with the files that are to be scanned" (Col. 3, lines 18-20 - emphasis added). However, a processor simply requesting data streams from a storage medium, as in Chi, fails to disclose "audit data generator logic separate from said computer virus scanner logic and being triggered by said computer virus scanner logic prior to said generating said scan result" (emphasis added), as claimed by appellant.

In addition, with respect to the independent claims, the Examiner has relied on Col. 3, lines 17-23 from Chi to make a prior art showing of appellant's claimed "identifying a request to execute a computer program associated with said computer file to be scanned for computer viruses by said computer virus scanner logic" (see this or similar, but not necessarily identical language in the independent claims).

Appellant respectfully asserts that such excerpt from Chi merely discloses that "the processor 110 receives a request to scan files for viruses" (Col. 3, lines 17-18 - emphasis added). Clearly, the mere disclosure of receiving a request to scan files for viruses fails to even suggest "identifying a request to **execute** a computer program associated with said computer file to be scanned for computer viruses by said computer virus scanner logic" (emphasis added), as claimed by appellant.

Furthermore, with respect to the independent claims, the Examiner has relied on Col. 5 lines 56-60; Col. 12, lines 38-43; and Col. 34, lines 45-62 from Farber to make a prior art showing of appellant's claimed "in response to identification of said request to execute said computer program, generating audit data identifying said computer program" (see this or similar, but not necessarily identical language in the independent claims).

Appellant respectfully asserts that the excerpts from Farber relied upon by the Examiner simply teach that "the system might store the True Names of all executable applications on the system and then periodically redetermine the True Names of each of these applications to ensure that they match the stored True Names" (Col. 34, lines 50-54 - emphasis added). Additionally, the

excerpts disclose a technique where "[t]he Verify True File mechanism verifies that a data item in a True File registry is indeed the correct data item given its True Name" (Col. 34, lines 60-62 - emphasis added). However, periodically re-determining and verifying True Names of executable applications simply fails to even suggest a technique where "in response to **identification of said** request to execute said computer program, audit data identifying said computer program [is generated]" (emphasis added), as claimed by appellant.

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be unobvious to combine the Chi and Farber references relied on by the Examiner, and since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claim 58

With respect to Claim 58, the Examiner has relied on Col. 7, lines 39-50 from Chi, and Col. 34, lines 45-62 from Farber to make a prior art showing of appellant's claimed technique "wherein said computer virus scanner logic generates said scan result after receiving a reply from said audit data generator logic."

Appellant respectfully asserts that the excerpt from Chi relied on by the Examiner merely teaches that "[t]o evaluate the Boolean expressions, the processor 110 retrieves from the system memory 140 the virus signature 430 to be evaluated and the scan results 420 indicating whether the components of the signature were detected in the scanned data streams" (Col. 7, lines 41-45 – emphasis added). Further, Chi discloses that "[t]he processor 110 stores intermediate evaluation results in an evaluation stack 410, located in the system memory 140" (Col. 7, lines 45-47). However, Chi's disclosure of a processor that retrieves a virus signature, and scan results indicating if the components of the signature were detected, fails to even suggest "receiving a reply from said audit data generator logic" (emphasis added), as claimed by appellant.

Furthermore, appellant respectfully asserts that the excerpt from Farber relied on by the Examiner merely teaches that "...data items in the system can be verified and have their integrity checked" (Col. 34, lines 45-47 – emphasis added). In addition, the excerpt teaches that "[t]his

can be used for security purposes, for instance, to check for viruses and to verify that data retrieved from another location is the desired...and requested data" (Col. 34, lines 47-50 – emphasis added). However, disclosing that data items in a system can have their integrity checked to verify whether data retrieved from another location is the requested data, fails to even suggest a technique "wherein said computer virus scanner logic generates said scan result after receiving a reply from said audit data generator logic" (emphasis added), as claimed by appellant.

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be unobvious to combine the references relied on by the Examiner, and since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #3: Claim 59

With respect to Claim 59, the Examiner has relied on Col. 7, lines 39-50 from Chi, and Col. 34, lines 45-62 from Farber to make a prior art showing of appellant's claimed technique "wherein said computer virus scanner logic generates said scan result as a function of a reply from said audit data generator logic."

Appellant respectfully points out that the Examiner states "Chi as modified teaches said computer virus scanner logic generates said scan result after receiving a reply from said audit data generator logic." However, appellant claims a technique "wherein said computer virus scanner logic generates said scan result as a function of a reply from said audit data generator logic" (emphasis added), as claimed by appellant.

Appellant respectfully asserts that the excerpt from Chi relied on by the Examiner merely teaches that in order "[t]o evaluate the Boolean expressions, the processor 110 retrieves from the system memory 140 the virus signature 430 to be evaluated and the scan results 420 indicating whether the components of the signature were detected in the scanned data streams" (Col. 7, lines 41-45 – emphasis added). Further, Chi discloses that "[t]he processor 110 stores intermediate evaluation results in an evaluation stack 410, located in the system memory 140" (Col. 7, lines 45-47).

However, Chi's disclosure of a processor that retrieves a virus signature and scan results indicating if the components of the signature were detected fails to mention "a reply from said audit data generator logic," much less a technique "wherein said computer virus scanner logic generates said scan result as a function of a reply from said audit data generator logic" (emphasis added), as claimed by appellant.

Furthermore, appellant respectfully asserts that the excerpt from Farber relied on by the Examiner merely teaches that "...data items in the system can be verified and have their integrity checked" (Col. 34, lines 45-47 – emphasis added). In addition, the excerpt teaches that "[t]his can be used for security purposes, for instance, to check for viruses and to verify that data retrieved from another location is the desired...and requested data" (Col. 34, lines 47-50 – emphasis added). However, disclosing that data items in a system can have their integrity checked to verify whether data retrieved from another location is the requested data, fails to even suggest a technique "wherein said computer virus scanner logic generates said scan result as a function of a reply from said audit data generator logic" (emphasis added), as claimed by appellant. Clearly, verifying and integrity checking data items, as in Farber, fails to meet "generat[ing] said scan result as a function of a reply from said audit data generator logic" (emphasis added), in the manner as claimed by appellant.

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be unobvious to combine the references relied on by the Examiner, and since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #4: Claim 60

With respect to Claim 60, the Examiner has relied on Col. 8, lines 43-48 from Chi to make a prior art showing of appellant's claimed "wherein a reply from said audit data generator logic is not used by said computer virus scanner logic if said scan result includes a failure."

Appellant respectfully asserts that the excerpt relied on by the Examiner merely teaches that "if the top stack value is false, the Boolean expression representing the virus signature is not

satisfied, and the processor 110 reports 570 the virus was not detected" (Col. 8, lines 43-45 - emphasis added). Clearly, disclosing that a processor reports that a virus was not detected if a Boolean expression of a virus signature is not satisfied, as in Chi, fails to even suggest a technique "wherein a reply from said audit data generator logic is not used by said computer virus scanner logic if said scan result includes a failure" (emphasis added), as claimed by appellant.

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be unobvious to combine the references relied on by the Examiner, and since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #5: Claim 61

With respect to Claim 61, the Examiner has relied on Col. 34, line 45-49 from Farber to make a prior art showing of appellant's claimed technique "wherein said data identifying said computer file is sent to said audit data generator logic prior to performing said computer virus scan."

Appellant respectfully asserts that the excerpt relied on by the Examiner merely teaches that "...data items in the system can be verified and have their integrity checked" (Col. 34, lines 45-46). In addition, the excerpt teaches that "[t]his can be used for security purposes, for instance, to check for viruses and to verify that data retrieved from another location is the desired...and requested data" (Col. 34, lines 47-50 – emphasis added). However, Farber's disclosure that data items in a system can have their integrity checked to verify whether data retrieved from another location is the desired data, fails to even suggest a technique "wherein said data identifying said computer file is sent to said audit data generator logic prior to performing said computer virus scan" (emphasis added), as claimed by appellant. Clearly, verifying and integrity checking data items in order to check for viruses, as in Farber, fails to suggest that "data identifying said computer file is sent to said audit data generator logic prior to performing said computer virus scan" (emphasis added), as claimed by appellant.

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be unobvious to combine the references relied on by the Examiner, and since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue # 5:

The Examiner has rejected Claims 2-5, 20-23, and 38-41 under 35 U.S.C. 103(a) as being unpatentable over Chi (U.S. Patent No. 6,006,329), in view of Farber et al. (U.S. Patent No. 6,415,280), in view of Greschler et al. (U.S. Publication No. 2002/0078203), and further in view of Chambers (U.S. Patent No. 5,398,196).

Group #1: Claims 2, 20, and 38

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #4, Group #1.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Group #2: Claims 3-5, 21-23 and 39-41

With respect to Claims 3, 21, and 39, the Examiner has relied on Col. 1, line 68 – Col. 2, line 10; and Col. 6, lines 41-50 from Chambers to make a prior art showing of appellant's claimed technique "wherein said audit data generator logic is responsive to data identifying one or more banned computer programs to identify a request to execute a banned computer program" (see this or similar, but not necessarily identical language in the claims listed above). Specifically, the Examiner has argued that "a banned program is interpreted as that not within a permitted program list."

Appellant respectfully disagrees, and asserts that the excerpts relied on by the Examiner merely teach that "[the earliest antivirus programs] would allow a virus program to execute in memory

but would intercept strategic operating system function requests made by the computer virus" (Col. 1, lines 66-Col. 2, line 1). In addition, the excerpts teach that "[t]he viral code would then execute, and at block 460 would determine if there was a file name associated with the operating system call" since "[s]uch operating system calls are typically used by a normal program to open a file or execute another program" (Col. 6, lines 40-44 - emphasis added).

First, appellant respectfully asserts that such excerpts from Chambers do not disclose a permitted program list, as noted by the Examiner. In addition, disclosing that operating system calls are typically used to open a file or execute another program, as in Chambers, in no way suggests "audit data generator logic [which] is responsive to data identifying one or more banned computer programs to identify a request to execute a banned computer program" (emphasis added), as claimed by appellant. Clearly, allowing a program to execute, as in Chambers, fails to meet "identify[ing] a request to execute a banned computer program" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Issue # 6:

The Examiner has rejected Claims 13, 14, 17, 18, 31, 32, 35, 36, 49, 50, 53, and 54 under 35 U.S.C. 103(a) as being unpatentable over Chi (U.S. Patent No. 6,006,329), in view of Farber et al. (U.S. Patent No. 6,415,280), in view of Greschler et al. (U.S. Publication No. 2002/0078203), and further in view of Hypponen et al. (U.S. Patent No. 6,577,920).

Group #1: Claims 13, 31, and 49

With respect to Claims 13, 31, and 49, the Examiner has relied on Col. 1, lines 47-53; Col. 1, lines 66-67; and Col. 3, lines 26-31 from Hypponen to make a prior art showing of appellant's claimed technique "wherein said audit data generator logic is responsive to a non-user specified database of data indicative of particular computer programs" (see this or similar, but not necessarily identical language in the foregoing claims).

Appellant respectfully asserts that the excerpts relied on by the Examiner merely teach "alerting a user in the event that the macro has a signature corresponding to a signature contained in said first database and/or in the event that the macro has a signature which does not correspond to a signature contained in either of the second and third databases" (Col. 3, lines 26-31 - emphasis added). However, merely disclosing that a macro signature is compared to other signatures in a database fails to even suggest a technique "wherein said audit data generator logic is responsive to a non-user specified database of data indicative of particular computer programs" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Group #2: Claims 14, 32, and 50

With respect to Claims 14, 32, and 50, the Examiner has relied on Col. 3, lines 3-10 from Hypponen to make a prior art showing of appellant's claimed technique "wherein said audit data generator logic is responsive to a user specified database of data indicative of particular computer programs" (see this or similar, but not necessarily identical language in the foregoing claims).

Appellant respectfully asserts that such excerpt from Hypponen merely teaches that "...the method comprises creating a set of signatures corresponding to a set of user specific macros, certified by the user as being virus free" (Col. 3, lines 3-5). In addition, the excerpt teaches that "...the method comprises scanning a macro identified in a file to determine whether or not the macro has a signature corresponding to a signature of a user certified macro" (Col. 3, lines 7-10). However, disclosing a database corresponding to a set of user specific macros that may be updated by a network manager, as in Hypponen, fails to even suggest a technique "wherein said audit data generator logic is responsive to a user specified database of data indicative of particular computer programs" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Group #3: Claims 17, 35, 53

Wirth respect to dependent Claims 17, 35, and 53, the Examiner has relied on Col. 5, lines 62-65 from Hypponen to make a prior art showing of appellant's claimed technique "wherein local audit data is stored upon a computer within a computer network until said computer is polled by a remote computer upon said computer network whereupon said local audit data is sent to said remote computer" (see this or similar, but not necessarily identical language in the foregoing claims).

Appellant respectfully asserts that the excerpt from Hypponen relied upon by the Examiner merely teaches that "a report is sent to the network manager 7, and also possibly to the remote server 17 of the software provider" (Col. 5, lines 62-63 - emphasis added). However, the mere disclosure of sending the report to a network manager or remote server fails to suggest a specific technique "wherein local audit data is stored upon a computer within a computer network until said computer is polled by a remote computer" (emphasis added), as claimed by appellant.

In addition, with respect to dependent Claims 17, 35, and 53, the Examiner has simply dismissed the same under Official Notice. Specifically, the Examiner has stated that it would have been obvious for one of ordinary skill in the art at the time the invention was made "[for a local computer] to be polled by a remote computer upon said computer network whereupon said local audit data is sent to said remote computer." Appellant respectfully disagrees. Further, appellant respectfully asserts that simply polling a local computer by a remote computer simply fails to specifically suggest that "local audit data is stored upon a computer within a computer network until said computer is polled by a remote computer" (emphasis added), as claimed by appellant.

Appellant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP below.

"If the appellant traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Group #4: Claims 18, 36, 54

With respect to Claims 18, 36, and 54, the Examiner has relied on Col. 5, lines 62-65 from Hypponen to make a prior art showing of appellant's claimed technique "wherein said remote computer generates a consolidated audit report for a plurality of computers upon said computer network" (see this or similar, but not necessarily identical language in the foregoing claims).

Appellant respectfully asserts that the excerpt relied on by the Examiner merely teaches that "a report is sent to the network manager 7, and also possibly to the remote server 17 of the software provider" and that '[t]his report may be accompanied by a copy of the "guilty" macro' (Col. 5, lines 62-65). However, merely disclosing that a report is sent if the identified macro signature is not found in the database, does not suggest a technique "wherein said remote computer generates a consolidated audit report for a plurality of computers upon said computer network" (emphasis added), as claimed by appellant. Clearly, a report with a copy of the guilty macro fails to suggest "a consolidated audit report" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Issue # 7:

The Examiner has rejected Claims 17, 18, 35, 36, 53, and 54 under 35 U.S.C. 103(a) as being unpatentable over Chi (U.S. Patent No. 6,006,329), in view of Farber et al. (U.S. Patent No. 6,415,280), in view of Greschler et al. (U.S. Publication No. 2002/0078203), and further in view of Schlossberg et al. (U.S. Publication No. 2002/0066034).

Group #1: Claims 17, 35, 53

With respect to dependent Claims 17, 35, and 53, the Examiner has relied on paragraphs [0009] and [0061] in Schlossberg to make a prior art showing of appellant's claimed technique "wherein local audit data is stored upon a computer within a computer network until said computer is polled by a remote computer upon said computer network whereupon said local audit data is sent to said remote computer."

Appellant respectfully asserts that the excerpts from Schlossberg relied upon by the Examiner merely disclose that "[t]he Interception Unit 103 or Detection Units 105 can be installed on all sub-networks, which are networks of users and servers connected to the main protected network, in the protected network to monitor the traffic on the entire sub-network" (paragraph [0061] - emphasis added). Further, Schlossberg discloses that "[t]hese units are constantly polled by the Management Unit 117" (paragraph [0061] - emphasis added). Clearly, the mere disclosure in Schlossberg that the Interception Unit and Detection Units are constantly polled by the Management Unit fails to even suggest that "local **audit data** is stored upon a computer within a computer network **until** said computer is polled by a remote computer" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Group #2: Claims 18, 36, 54

With respect to Claims 18, 36, and 54, the Examiner has relied on element 709 of Figure 7 from Schlossberg to make a prior art showing of appellant's claimed technique "wherein said remote computer generates a consolidated audit report for a plurality of computers upon said computer network."

Appellant respectfully asserts that element 709 in Figure 7 from Schlossberg merely indicates that "if the attacker's activities match a Boolean logic table entry indicating that a report needs to be made, the sensor unit packages the data on the attacker's activities into a message which is

sent via the network using an encrypted message protocol, step 709 (Schlossberg, Paragraph [0079] – emphasis added). However, Schlossberg's mere disclosure of generating a report if an attacker's activities match a Boolean logic table entry, and that the data on the attacker's activities is packaged into a message, fails to suggest a technique "wherein said remote computer generates a consolidated audit report for a plurality of computers" (emphasis added), as claimed by appellant. Clearly, packaging data on the attacker's activities into a message fails to meet "generat[ing] a consolidated audit report for a plurality of computers" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Issue # 8:

The Examiner has rejected Claims 16, 34, and 52 under 35 U.S.C. 103(a) as being unpatentable over Chi (U.S. Patent No. 6,006,329), in view of Farber et al. (U.S. Patent No. 6,415,280), in view of Greschler et al. (U.S. Publication No. 2002/0078203),, and further in view of Bates et al. (U.S. Patent No. 6,721,721).

Group #1: Claims 16, 34, and 52

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #4, Group #1.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A computer program product comprising a computer program operable to control a computer to generate audit data indicative of a request to execute a computer program, said computer program comprising:

(i) computer virus scanner logic, responsive to a computer virus scan request including data identifying a computer file to be scanned for computer viruses, for performing a computer virus scan and for generating a scan result;

(ii) audit data generator logic separate from said computer virus scanner logic and being triggered by said computer virus scanner logic prior to said generating said scan result, and responsive to said data identifying said computer file to be scanned that is received from said computer virus scanner logic for simultaneously performing additional operations in parallel with said computer virus scan, said additional operations including
identifying a request to execute a computer program associated with said computer file to be scanned for computer viruses by said computer virus scanner logic and, in response to identification of said request to execute said computer program, generating audit data identifying said computer program; and

(iii) concurrent usage logic for performing a concurrent usage check for identifying a request to execute a further computer program that would result in said further computer program concurrently executing upon more than a predetermined number of computers upon a computer network;

wherein said predetermined number varies with time.

2. (Original) A computer program product as claimed in claim 1, wherein a file access request to an operating system triggers generation of said computer virus scan request.

3. (Original) A computer program product as claimed in claim 1, wherein said audit data generator logic is responsive to data identifying one or more banned computer programs to identify a request to execute a banned computer program.

4. (Original) A computer program product as claimed in claim 3, wherein, if a request to execute a banned computer program is identified, then one or more banned program actions are triggered, said banned program actions including one or more of:

(i) said banned computer program is deleted;

(ii) said banned computer program is disabled;

(iii) said banned program is encrypted and replaced by a stub program; and

(iv) an alert indicating detection of said banned computer program is issued.

5. (Original) A computer program product as claimed in claim 3, wherein said data identifying one or more banned computer programs is a permitted computer program list with any computer program not included within said permitted computer program list being a banned computer program.

6. (Cancelled)

7. (Previously Presented) A computer program product as claimed in claim 1, wherein, if said concurrent usage check indicates that said request to execute said further computer program would result in more than said predetermined number of computers upon said computer network concurrently executing said computer program, then said request to execute said further computer program is denied.

8. (Previously Presented) A computer program product as claimed in claim 7, wherein a user message is displayed when execution of said further computer program is prevented.

9. (Cancelled)

10. (Previously Presented) A computer program product as claimed in claim 1, wherein at certain times said predetermined number is zero.

11. (Original) A computer program product as claimed in claim 1, wherein said audit data generator logic calculates a checksum value from said computer file, said checksum value being used in identification of said computer file as a particular computer program.

12. (Original) A computer program product as claimed in claim 11, wherein said audit data generator logic stores said calculated checksum value and uses said stored calculated checksum values instead of recalculating said checksum value when said computer file subject to a subsequent access without any intervening change having been made to said computer file.

13. (Original) A computer program product as claimed in claim 1, wherein said audit data generator logic is responsive to a non-user specified database of data indicative of particular computer programs.

14. (Original) A computer program product as claimed in claim 1, wherein said audit data generator logic is responsive to a user specified database of data indicative of particular computer programs.

15. (Original) A computer program product as claimed in claim 1, wherein said computer virus scan request results from an on-access scan.

16. (Original) A computer program product as claimed in claim 1, wherein said computer virus scan request results from an on-demand scan.

17. (Original) A computer program product as claimed in claim 1, wherein local audit data is stored upon a computer within a computer network until said computer is polled by a remote computer upon said computer network whereupon said local audit data is sent to said remote computer.

18. (Original) A computer program product as claimed in claim 17, wherein said remote computer generates a consolidated audit report for a plurality of computers upon said computer network.

19. (Previously Presented) A method of generating audit data indicative of a request to execute a computer program, said method comprising the steps of:

(i) responsive to a computer virus scan request within a computer virus scanner, performing a computer virus scan and generating a scan result, said computer virus scan request including data identifying a computer file to be scanned for computer viruses;

(ii) triggering operation of an audit data generator which is separate from said computer virus scanner, using said computer virus scanner prior to said generating said scan result, said audit data generator being responsive to said data identifying said computer file to be scanned that is received from said computer virus scanner for simultaneously performing additional operations in parallel with said computer virus scan, said additional operations including identifying a request to execute a computer program associated with said computer file to be scanned for computer viruses by said computer virus scanner;

(iii) in response to identification of said request to execute said computer program, generating audit data identifying said computer program; and

(iv) performing a concurrent usage check for identifying a request to execute a further computer program that would result in said further computer program concurrently executing upon more than a predetermined number of computers upon a computer network;

wherein said predetermined number varies with time.

20. (Original) A method as claimed in claim 19, wherein a file access request to an operating system triggers generation of said computer virus scan request.

21. (Original) A method as claimed in claim 19, wherein said audit data generator is responsive to data identifying one or more banned computer programs to identify a request to execute a banned computer program.

22. (Original) A method as claimed in claim 21, wherein, if a request to execute a banned computer program is identified, then one or more banned program actions are triggered, said banned program actions including one or more of:

(i) said banned computer program is deleted;

(ii) said banned computer program is disabled;

(iii) said banned program is encrypted and replaced by a stub program; and

(iv) an alert indicating detection of said banned computer program is issued.

23. (Original) A method as claimed in claim 21, wherein said data identifying one or more banned computer programs is a permitted computer program list with any computer program not included within said permitted computer program list being a banned computer program.

24. (Cancelled)

25. (Previously Presented) A method as claimed in claim 19, wherein, if said concurrent usage check indicates that said request to execute said further computer program would result in more than said predetermined number of computers upon said computer network concurrently executing said further computer program, then said request to execute said further computer program is denied.

26. (Previously Presented) A method as claimed in claim 25, wherein a user message is displayed when execution of said further computer program is prevented.

27. (Cancelled)

28. (Previously Presented) A method as claimed in claim 19, wherein at certain times said predetermined number is zero.

29. (Original) A method as claimed in claim 19, wherein said audit data generator calculates a checksum value from said computer file, said checksum value being used in identification of said computer file as a particular computer program.

30. (Original) A method as claimed in claim 29, wherein said audit data generator stores said calculated checksum value and uses said stored calculated checksum values instead of recalculating said checksum value when said computer file subject to a subsequent access without any intervening change having been made to said computer file.

31. (Original) A method as claimed in claim 19, wherein said audit data generator is responsive to a non-user specified database of data indicative of particular computer programs.

32. (Original) A method as claimed in claim 19, wherein said audit data generator is responsive to a user specified database of data indicative of particular computer programs.

33. (Original) A method as claimed in claim 19, wherein said computer virus scan request results from an on-access scan.

34. (Original) A method as claimed in claim 19, wherein said computer virus scan request results from an on-demand scan.

35. (Original) A method as claimed in claim 19, wherein local audit data is stored upon a computer within a computer network until said computer is polled by a remote computer upon said computer network whereupon said local audit data is sent to said remote computer.

36. (Original) A method as claimed in claim 35, wherein said remote computer generates a consolidated audit report for a plurality of computers upon said computer network.

37. (Previously Presented) Apparatus for generating audit data indicative of a request to execute a computer program, said apparatus comprising:

(i) a computer virus scanner, responsive to a computer virus scan request, for performing a computer virus scan and for generating a scan result, said computer virus scan request including data identifying a computer file to be scanned for computer viruses;

(ii) an audit data generator separate from said computer virus scanner and being triggered by said computer virus scanner prior to said generating said scan result, and responsive to said data identifying said computer file to be scanned that is received from said computer virus scanner for simultaneously performing additional operations in parallel with said computer virus scan, said additional operations including

identifying a request to execute a computer program associated with said computer file to be scanned for computer viruses by said computer virus scanner and, in response to identification of

said request to execute said computer program, generating audit data identifying said computer program; and

concurrent usage monitor for performing a concurrent usage check for identifying a request to execute a further computer program that would result in said further computer program concurrently executing upon more than a predetermined number of computers upon a computer network;

wherein said predetermined number varies with time.

38. (Original) Apparatus as claimed in claim 37, wherein a file access request to an operating system triggers generation of said computer virus scan request.

39. (Original) Apparatus as claimed in claim 37, wherein said audit data generator is responsive to data identifying one or more banned computer programs to identify a request to execute a banned computer program.

40. (Original) Apparatus as claimed in claim 39, wherein, if a request to execute a banned computer program is identified, then one or more banned program actions are triggered, said banned program actions including one or more of:

(i) said banned computer program is deleted;

(ii) said banned computer program is disabled;

(iii) said banned program is encrypted and replaced by a stub program; and

(iv) an alert indicating detection of said banned computer program is issued.

41. (Original) Apparatus as claimed in claim 39, wherein said data identifying one or more banned computer programs is a permitted computer program list with any computer program not included within said permitted computer program list being a banned computer program.

42. (Cancelled)

43. (Previously Presented) Apparatus as claimed in claim 37, wherein, if said concurrent usage check indicates that said request to execute said further computer program would result in

more than said predetermined number of computers upon said computer network concurrently executing said further computer program, then said request to execute said further computer program is denied.

44. (Previously Presented) Apparatus as claimed in claim 43, wherein a user message is displayed when execution of said further computer program is prevented.

45. (Cancelled)

46. (Previously Presented) Apparatus as claimed in claim 37, wherein at certain times said predetermined number is zero.

47. (Original) Apparatus as claimed in claim 37, wherein said audit data generator calculates a checksum value from said computer file, said checksum value being used in identification of said computer file as a particular computer program.

48. (Original) Apparatus as claimed in claim 47, wherein said audit data generator stores said calculated checksum value and uses said stored calculated checksum values instead of recalculating said checksum value when said computer file subject to a subsequent access without any intervening change having been made to said computer file.

49. (Original) Apparatus as claimed in claim 37, wherein said audit data generator is responsive to a non-user specified database of data indicative of particular computer programs.

50. (Original) Apparatus as claimed in claim 37, wherein said audit data generator is responsive to a user specified database of data indicative of particular computer programs.

51. (Original) Apparatus as claimed in claim 37, wherein said computer virus scan request results from an on-access scan.

52. (Original) Apparatus as claimed in claim 37, wherein said computer virus scan request results from an on-demand scan.

53. (Original) Apparatus as claimed in claim 37, wherein local audit data is stored upon a computer within a computer network until said computer is polled by a remote computer upon said computer network whereupon said local audit data is sent to said remote computer.

54. (Previously Presented) Apparatus as claimed in claim 53, wherein said remote computer generates a consolidated audit report for a plurality of computers upon said computer network.

55.-57. (Cancelled)

58. (Previously Presented) A computer program product as claimed in claim 1, wherein said computer virus scanner logic generates said scan result after receiving a reply from said audit data generator logic.

59. (Previously Presented) A computer program product as claimed in claim 1, wherein said computer virus scanner logic generates said scan result as a function of a reply from said audit data generator logic.

60. (Previously Presented) A computer program product as claimed in claim 1, wherein a reply from said audit data generator logic is not used by said computer virus scanner logic if said scan result includes a failure.

61. (Previously Presented) A computer program product as claimed in claim 1, wherein said data identifying said computer file is sent to said audit data generator logic prior to performing said computer virus scan.

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

N/A

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P456/00.163.01).

Respectfully submitted,

By: _____ Date: 11/22/06

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660